UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/620,108	07/15/2003	Marcus Janke	S&ZIO020101	8615

24131 7590 04/10/2007

LERNER GREENBERG STEMER LLP
P O BOX 2480
HOLLYWOOD, FL 33022-2480

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/620,108	JANKE, MARCUS	
	Examiner	Art Unit	
	Zachary A. Davis	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20030715, 20031215, 20050720*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A preliminary amendment was received on 10 November 2003. By this amendment, Claim 2 has been amended. No claims have been added or canceled. Claims 1-16 are currently pending in the present application.

Specification

2. The disclosure is objected to because of the following informalities:

The specification appears to contain minor typographical and other errors. For example, reference is made in the abstract and throughout the specification and claims to an "energy interface", "supply energy", and similar phrases. This is uncommon usage of the term "energy"; it appears that "power" is the term that is intended. Further, throughout the specification, it is noted that the line numbers begin with line 5 on each page. Other specific examples include:

On page 1, line 30, the phrase "the increasing information-technological networking" is generally vague. On page 1, line 37, it appears that "DSE" is intended to read "DES". On page 3, line 16, in the phrase "a by far greater change of success", it appears that "by" should be deleted. On page 3, lines 31-33, in the phrase "on the other hand increase also the circuitry and design expenditure", the placement of the word "also" is generally awkward. On page 4, lines 14-15 and 31-32; page 5, lines 15-16 and 33-34; and page 6, lines 13-14, in the phrase "this aspect is achieved", it appears that

"aspect" is intended to read "object". On page 5, lines 18-19, it appears that the reference to an energy interface is instead intended to refer to a data interface, since data is received. On page 7, line 31, the phrase "The not received remainder" is generally awkwardly worded. On page 9, line 8, the phrase "performing in the scope of specific attacks" is generally unclear. On page 9, lines 22-24, the phrase "whereby it is further aggravated for a potential attacker to adjust to, or find out, the algorithm code employed" is generally narrative and unclear. On page 9, line 30, it appears that "EC cards" is intended to read "IC cards". On page 11, lines 5 and 12, it is not clear what exactly is referred to by "plug-in cards" and "plug-in spaces". On page 12, line 12, it appears that "chard" is intended to read "card". On page 13, lines 25-26, the phrase "the chip card 10 does not longer carry out processings" is generally unclear, particularly in the phrasing "does not longer" and the use of the term "processings". On page 13, lines 39-40, it is not clear what the subject of the phrase "before performing by a cryptographic processor" is. On page 14, line 12, reference is made to "the DES standard"; however, it is noted that this is redundant, as the "S" in "DES" stands for "standard". On page 15, lines 7-11, the phrase beginning "For preventing attempts of potential attackers to protect the volatile memory" is generally unclear and narrative. On page 20, lines 25 and 29, the use of the word "already" is generally unclear.

Appropriate correction is required. The lengthy specification has not been checked to the extent necessary to determine the presence of all possible minor errors. The above is not to be considered an exhaustive list of errors. Applicant's cooperation

is requested in correcting any errors of which applicant may become aware in the specification.

Claim Objections

3. Claims 1, 11, and 13-15 objected to because of the following informalities:

Claims 1, 11, and 13-15 each include limitations such as "energy interface" and "supply energy" and similar phrases. This is uncommon usage for the term "energy"; it appears that "power" is intended.

In Claim 1, at lines 4-5 of the claim, it appears that in the phrase "receiving at least part of an algorithm code or of the complete algorithm code", it appears that the second "of" (after the "or") should be deleted.

In Claim 11, the limitation beginning "volatile-storing" ends with a colon; it appears that this should be replaced by a semicolon.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-16 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "the same" in line 13 of the claim. It is not clear what the antecedent of this phrase is; although it appears that it is intended to be the volatile memory, it appears that this could also refer to the energy interface.

Claim 2 recites the limitation "the non-received remainder of the algorithm code is stored". This is generally vague and unclear. First, the phrase "non-received" is generally unclear, and second, if the code is "non-received" then it is not clear how it is possible to store it.

Each of Claims 4-10 recites "A security module according to any of claim 1". This is generally unclear, as it is not explicitly clear from which claim or claims these claims are intended to depend. For purposes of interpreting the claims, it has been assumed that each of Claims 4-10 depends from Claim 1.

Claim 4 further recites the limitation "said part of the algorithm code or the complete algorithm code in encrypted form and/or a certificate". The use of the conjunctions in this phrase is generally unclear, as it is not clear which of these are required to be received. In particular, the use of "and/or" is unclear for the same reason. The claim further recites "examining the certificate" but does not specify the manner in which it is examined or, more particularly, what aspects of the certificate are examined. Additionally, the phrase "said certificate lacks genuineness" is generally unclear.

Claim 5 recites the limitation "the transferred part of the algorithm code". There is insufficient antecedent basis for this limitation in the claims.

Claim 6 recites the limitation "selected from a plurality of conditions comprising..." This is not a proper Markush claim, because it uses "comprising" instead of "consisting of". Therefore, it does not clearly set forth all of the possible alternatives encompassed by the claims. It is uncertain what the scope of the claims is. See MPEP § 2173.05(h) I. Further, the phrase "as well as of additional operating parameters" renders the claim indefinite because the claim includes elements not actually disclosed (those encompassed by "additional parameters"), thereby rendering the scope of the claim unascertainable. See MPEP § 2173.05(d). Additionally, it is not clear what exactly is encompassed by the terms "irregularity" and "fluctuation".

Claim 7 recites the limitation "selected from a group comprising..." This is not a proper Markush claim, because it uses "comprising" instead of "consisting of". Therefore, it does not clearly set forth all of the possible alternatives encompassed by the claims. It is uncertain what the scope of the claims is. See MPEP § 2173.05(h) I. Further, the phrase "an access function for accessing" is generally non-descriptive and unclear, as it is not clear what is accessed, and without further description it is redundant in that an access function inherently is "for accessing". Additionally, the phrase "as well as an access function for changing" is unclear because the use of "as well as" makes it unclear whether the access function for changing is a part of the group from which the task is selected. Finally, it is unclear exactly what is meant by "a value stored on the security module".

Claim 8 recites the limitation "the part received of the algorithm code". However, this is unclear because either a part of the code or an entire algorithm code can be received; it is not clear how this is further limiting when the entire code is received. Additionally, the phrase "jump addresses" is generally unclear, not having been defined in the specification nor having a clearly established meaning in the art.

Claim 9 recites the limitation "storing a newly received, altered part of the algorithm code over the stored part of the algorithm code or the stored complete algorithm code". The use of the preposition "over" is generally vague, since what is stored is not a physical object. Further, it is not clear how a (newly received) part of the algorithm code could be stored over the complete algorithm code if the part, assumedly, is smaller than the complete code.

Claim 11 recites receiving algorithm code "by means of an energy interface". This would appear to be impossible. For purposes of interpreting the claims, it is assumed that this is intended to read "by means of a data interface". The claim further recites "volatile-storing"; this is generally awkward and unclear. The claim also recites the limitation "the same" in line 9 of the claim. It is not clear what the antecedent of this phrase is; although it appears that it is intended to be the volatile memory, it appears that this could also refer to the energy interface. Additionally, the claim recites the limitation "the terminal". There is insufficient antecedent basis for this limitation in the claim.

Claim 12 recites "said step of clearing". Although this appears to refer to the last step of the process of Claim 11, it also appears that it could refer to the clearing referred to at line 10 of Claim 11.

Claim 13 recites the limitations "the algorithm code result" in lines 6-7 of the claim and "the further communication process" in line 20 of the claim. There is insufficient antecedent basis for these limitations in the claim. Further, the claim recites the limitation "the same" in line 11 of the claim. It is not clear what the antecedent of this phrase is; although it appears that it is intended to be the volatile memory, it appears that this could also refer to the energy interface or the supply energy. Additionally, the limitation beginning "with the terminal..." is generally unclear. For example, it is not clear what is meant by the phrase "during one and the same communication operation", nor is it clear what the subject of the phrase beginning "being designated" is. Further, the limitation beginning "subsequently" is generally unclear, as it is not clear what the subject of this limitation is, nor is it clear how this is a structural limitation of the claimed terminal.

Claim 14 recites the limitation "comprising for each communication operation". This is generally unclear. The claim also recites the limitation "during one and the same communication operation". It is not clear what is meant by this phrase. Further, the claim recites the limitation "the same" in line 13 of the claim. It is not clear what the antecedent of this phrase is; although it appears that it is intended to be the volatile memory, it appears that this could also refer to the energy interface or the supply

energy. Finally, the claim recites the limitation "the algorithm code result". There is insufficient antecedent basis for this limitation in the claim.

Claim 15 recites the phrase "volatile-storing"; this is generally awkward and unclear. The claim further recites the limitation "the supply energy" in lines 9-10 of the claim. There is insufficient antecedent basis for this limitation in the claims. Additionally, the claim recites the limitation "the same" in line 10 of the claim. It is not clear what the antecedent of this phrase is; although it appears that it is intended to be the volatile memory, it appears that this could also refer to the supply energy of the part of the algorithm code or complete algorithm code.

Claim 16 recites the phrase "repeated transferring of a plurality of different versions". First, the phrasing "repeated transferring" is generally vague and awkward. Further, it is not clear whether the same plurality of versions is transferred repeatedly, or if a single different version is transferred each of a plurality of times, or if a different plurality of different versions is transferred each of a plurality of times. The claim further recites the limitation "the repeatedly transferred version of said part of the algorithm code or of the complete algorithm code". There is insufficient antecedent basis for this limitation in the claims. Additionally, in the phrase "storing the repeatedly transferred version of said part of the algorithm code or of the complete algorithm code over the stored part of the algorithm code or over the complete stored algorithm code", the use of the preposition "over" is generally vague, since what is stored is not a physical object. Further, it is not clear how a part of the algorithm code could be stored over the complete algorithm code if the part, assumedly, is smaller than the complete code, or

conversely, how a complete algorithm code could be stored over a part of the algorithm code as there may not be sufficient space for the larger complete algorithm code.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-16 are rejected under 35 U.S.C. 102(b) as being anticipated by Schneier et al, US Patent 5768382.

In reference to Claim 1, Schneier discloses a security module including a data interface that receives, from a terminal, algorithm code concerning a processing of secrets (column 14, lines 19-21); an interface for receiving power (Figure 4D, power 27); a volatile memory storing the received algorithm code, where the volatile memory is cleared when the power supply is interrupted (Figure 4D, volatile memory 23b; column 14, lines 22-26); and a processor for performing the algorithm code (Figure 4C, CPU 302; column 11, lines 55-57).

In reference to Claim 2, Schneier further discloses non-volatile memory (column 14, lines 17-19).

In reference to Claim 3, Schneier further discloses means for performing authentication (column 20, lines 15-26).

In reference to Claim 4, Schneier further discloses receiving a certificate and examining a certificate, and decrypting code (column 14, lines 17-26; column 44, lines 30-35; column 50, lines 36-37).

In reference to Claims 5 and 8, Schneier further discloses a memory managing unit and code that includes addresses (column 7, lines 48-61).

In reference to Claim 6, Schneier further discloses means for monitoring a predetermined security condition and clearing the volatile memory if the condition is fulfilled (column 14, lines 19-26).

In reference to Claim 7, Schneier further discloses that the algorithm code can perform a symmetric cryptographic algorithm such as DES or an asymmetric cryptographic algorithm such as RSA (see column 9, line 58-column 10, line 11, and column 10, lines 27-40).

In reference to Claim 9, Schneier further discloses updating the code (column 14, lines 27-34).

In reference to Claim 10, Schneier further discloses a chip card (column 11, lines 34-44; column 7, lines 38-41; column 12, lines 6-44).

Claims 11 and 12 are directed to a method corresponding substantially to the module of Claim 1, and are rejected by a similar rationale.

In reference to Claim 13, Schneier discloses a terminal including a data interface that transmits, to a volatile memory in a security module, algorithm code concerning a processing of secrets (column 14, lines 19-21; Figure 4D, volatile memory 23b) and an interface for supplying power such that the volatile memory is cleared if there is an interruption in the power supply (Figure 4D, power 27; column 14, lines 22-26).

Claim 14 is directed to a method corresponding substantially to the terminal of Claim 13, and is rejected by a similar rationale.

Claim 15 is directed to a method encompassing the performance of the methods of Claims 11 and 14 simultaneously, and is rejected by a similar rationale. Claim 16 recites limitations corresponding to those recited in Claim 9, and is rejected by a similar rationale.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Matyas et al, US Patent 5103478, discloses a secure system in which cryptographic algorithms are stored in volatile memory (i.e. RAM).

b. Park, US Patent 5757909, discloses a secure system in which a smart card includes a RAM storing key information and an algorithm memory storing an encryption algorithm.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571) 272-3870. The examiner can normally be reached on weekdays 8:30-6:00, alternate Fridays off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

ZAD
zad

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137